DRAWINGS

Formal Drawings

The indication by the Examiner in the recent Office Action that the formal drawings filed with the application were approved by the Draftsman is noted with appreciation.

REMARKS/ARGUMENTS

Status

Claims 23-38 have been cancelled and claims 54-68 have been added. Claims 1-22 and 39-66, including independent claims 1, 16,, 39, and 54 will remain for further consideration.

More Clearly Defined

The claims in this application have been revised to voluntarily further clarify Applicant's unique invention. Applicant maintains that the claims as filed were patentable over the art of record. However, to expedite issuance of this application, reconsideration of the claims in light of the amendments and for the following reasons is respectfully requested.

Claim History

The Examiner rejected claims 1, 3, 12-14, 16, 24, 25 under 35 U.S.C. § 102 as being anticipated by Owens et al. The Examiner rejected claims 2, 4, 17, 27, 28, 37-42, 50 and 51 under 35 U.S.C. § 103 over Owens et al. in view of Blumenau.

35 U.S.C. § 102

The Examiner rejected claims 1, 3, 12-14, 16, 24, 25 under 35 U.S.C. § 102 as being anticipated by Owens et al. This rejection is respectfully traversed. The present invention is to a secure computer network link for sending data and information which is encrypted through an intermediate system which handles the handshaking and

authentication so that the end users only need be compatible with an intermediate system and do not need to have a separate protocol and direct access to various third party networks which may all carry their own cryptographic schemes.

The Owens et al. patent by contrast is to a method of identifying a user of a wireless network. The "cryptography" of the Owens patent merely involves taking a time varying input and a cryptographic key corresponding to the transmitted device idand processing the two in an algorithm to get a "dynamic personal identification number." There is no disclosure that the key is a "public-private key pair." The cryptographic key is always retrieved from a table based on the device identification number (as opposed to the calculated dynamic personal identification number" and not "decrypted." See col. 9mlines 28-35 and 42-50. Both systems appear to run the same encryption and compare that they both achieve the same result by "perform[ing] the personal identification compare step." Id. There is no reason to have a encryption "pair" since both systems are using the same encryption of the same inputs to compare the output of each.

Additionally, the Owens et al. system does not result in a "cryptographically secure network connection." The Owens et al. patent merely uses the dynamic person id number to verify log on, it does not use the cryptography to transmit data securely between the parties. See Figure 7 and ¶68 of the present application for a description of a description of a cryptographically secure network. Notably, in Figure 7, which describes the secure network, the authentication has already occurred and it is the transmission of the encrypted data which is makes the network cryptographically secure. Additionally, claim 1 recites two cryptographically secure network connections, the Owens et al. patent would only have one "connection" which is secure as the entire network of Owens et al. would

have a similar, symmetric connection throughout and between all of the telephones so that they can share data amongst the different telephones.

Newly added claim 54 further recited details of the use of a public key pair to authenticate the first and second access systems. The claim further recites that the transmission of data across the secure network uses a key pair to encrypt the data. Claims 62 and 63 recite that the authentication of each access system is performed using its own private-public key pair. Claims 64-66 recite that the transmission of data from the first access to the switch system use the first access system's public-private key pair and data from the second access system to the switch system use the second access system's public-private key pair. Claim 67 claims that each access system has a unique public-private key pair. None of these is shown in the Owens et al. patent.

For at least these reasons, the claims should be allowed over the art of record.

35 U.S.C. § 103

The Examiner rejected claims 2, 4, 17, 27, 28, 37-42, 50 and 51 under 35 U.S.C. § 103 over Owens et al. in view of Blumenau. However, Blumenau is again not analogous to the current invention and should not be considered. Further, Blumenau does not cure the defect of Owens et al., mainly that there is no key "pair." Blumenau specifically says in column 37 that there is no need to have a "pair" as only one encryption operation is used and "the private key would not be used." Therefore, there is no reason or motivation in Blumenau to switch to a public/private key pair since only one key is used, and certainly there is no teaching of authenticating using both the private and public key of a key pair.

For at least these reasons, the claims should be allowed over the art of record.

Summary

Applicants have made a diligent and bona fide effort to answer each and every ground for rejection or objection to the specification including the claims and to place the application in condition for final disposition. Reconsideration and further examination is respectfully requested, and for the foregoing reasons, Applicant respectfully submits that this application is in condition to be passed to issue and such action is earnestly solicited. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Robert N. Blackmon, Applicants' Attorney at 703-684-5633 to satisfactorily conclude the prosecution of this application.

Dated: September 30, 2005

Respectfully submitted,

Merek, Blackmon & Voorhees, LLC
673 S. Washington St.
Alexandria, Virginia 22314
Tel. 703-684-5633
Fax. 703-684-5637
E-mail: RNB@ BlackmonLaw.com

Robert N. Blackmon
Reg. No. 39494
Attorney/Agent for Applicant(s)

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.